(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-72721
(P2004-72721A)
(43)公開日　平成16年3月4日(2004.3.4)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	675A	5J104
G09C	1/00	G09C	1/00	640E	
H04L	9/08	H04L	9/00	601B	

審査請求 未請求　請求項の数 15　OL　（全 28 頁）

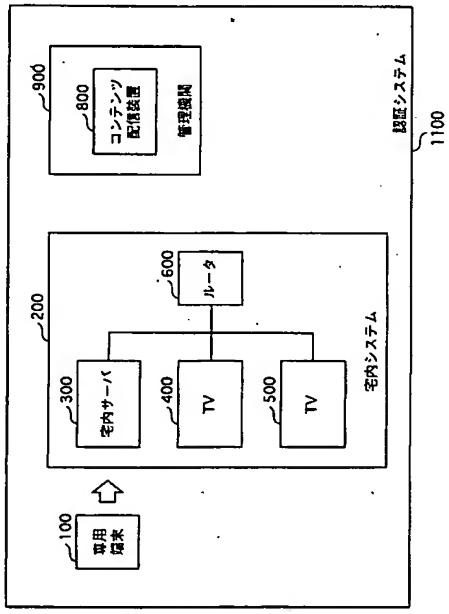
(21)出願番号　特願2003-151473(P2003-151473)
(22)出願日　平成15年5月28日(2003.5.28)
(31)優先権主張番号　特願2002-170251(P2002-170251)
(32)優先日　平成14年6月11日(2002.6.11)
(33)優先権主張国　日本国(JP)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(72)発明者　松崎　なつめ
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　舘林　誠
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　横田　薫
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】認証システム、鍵登録装置及び方法

(57)【要約】
【課題】コンテンツをユーザ宅内での個人使用に限定するために、ユーザ宅内の機器を簡易に設定することが可能な、認証システム及び鍵登録装置を提供することを目的とする。
【解決手段】第１機器と第２機器との間において、認証を行う認証システムである。前記第２機器は、当該第２機器に固有の識別子から、所定の鍵生成アルゴリズムに基づいて生成された第２鍵情報を記憶している。鍵登録装置は、前記識別子の入力を受け付け、前記鍵生成アルゴリズムに基づいて第１鍵データを生成し、前記第１機器に送信する。前記第１機器は、前記第１鍵データを受信して記憶する。
前記第１機器は、前記第２機器と通信する際、前記第１鍵データを用いて認証し、前記第２機器は、第２鍵データを用いて認証を受ける。
この構成により、鍵データを登録された機器以外と通信することを防ぐ。また、外部への接続手段を持たない機器でも実現できる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
第１機器と第２機器との間において、認証を行う認証システムであって、
前記第２機器に固有の識別子の入力を受け付け、所定の鍵生成アルゴリズムに基づいて前記識別子から第１鍵データを生成し、生成した第１鍵データを前記第１機器に送信する鍵登録装置と、
前記鍵登録装置から前記第１鍵データを受信して記憶し、当該第１鍵データを用いて前記第２機器を認証する第１機器と、
前記識別子から前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成される第２鍵データを予め記憶しており、前記第２鍵データを用いて前記第１機器による認証を受ける第２機器と
から構成されることを特徴とする認証システム。
【請求項２】
第１機器と第２機器との間において、認証を行う認証システムであって、
前記第２機器に固有の機器識別子の入力を受け付け、鍵生成アルゴリズムに基づいて前記機器識別子から第１鍵データを生成し、生成した第１鍵データを前記第１機器に送信する鍵登録装置と、
前記鍵登録装置から受信する前記第１鍵データを記憶し、前記第１鍵データを用いて前記第２機器を認証する第１機器と、
前記機器識別子からそれぞれ異なる鍵生成アルゴリズムに従って生成される複数の鍵データを予め記憶しており、前記複数の鍵データの内、前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第２鍵データを選択し、選択した第２鍵データを用いて、前記第１機器による認証を受ける第２機器と
から構成されることを特徴とする認証システム。
【請求項３】
前記第１機器は、更に、鍵登録装置の無効化を管理する管理機関により生成され、前記鍵登録装置の無効化を示す鍵無効化情報を受け取り、前記鍵登録装置から受信した第１鍵データを無効化し、
前記第２機器は、前記鍵無効化情報を受け取り、前記第２鍵データを無効化する
ことを特徴とする請求項２記載の認証システム。
【請求項４】
前記認証システムは、更に、鍵再登録装置を含み、
前記鍵再登録装置は、前記第２機器に固有の機器識別子の入力を受け付け、前記鍵登録装置の鍵生成アルゴリズムと異なる鍵生成アルゴリズムに基づいて前記第２機器に固有な機器識別子から第３鍵データを生成し、生成した第３鍵データと前記機器識別子とを前記第１機器に送信し、
前記第１機器は、更に、前記鍵再登録装置から受信する前記第３鍵データ及び前記機器識別子を対応付けて記憶し、前記第３鍵データを用いて前記第２機器を認証し、
前記第２機器は、更に、前記複数の鍵データの内、前記第３鍵データを生成した鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第４鍵データを用いて、前記第１機器による認証を受ける
ことを特徴とする請求項３記載の認証システム。
【請求項５】
前記第１機器は、前記管理機関により生成され、無効化された鍵登録装置に固有の識別子を更に含む鍵無効化情報を受け取り、更に受け取った識別子を無効化識別子として記憶し、
鍵登録装置から、第１鍵データと共に、前記鍵登録装置に固有の識別子を受け取り、受け取った識別子が前記無効化識別子と一致するか否かを判断し、一致する場合、前記鍵登録装置から前記第１鍵データを受け取ることを拒否する
ことを特徴とする請求項３記載の認証システム。

【請求項６】
前記第１機器は、前記管理機関により生成され、前記鍵無効化情報に前記管理機関の署名を施して生成された署名データを更に含む前記鍵無効化情報を受け取り、
前記署名データを検証し、検証結果が成功であれば、前記識別子を無効化識別子として記憶する
ことを特徴とする請求項５記載の認証システム。
【請求項７】
第２機器が有する、第１機器と前記第２機器との間で認証を行うための第２鍵データと同一の第１鍵データを、前記第１機器に設定する鍵登録装置であって、
前記第２機器に固有の識別子の入力を受け付ける入力手段と、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第１鍵データを生成する鍵データ生成手段と、
生成した前記第１鍵データを前記第１機器へ出力する出力手段と
から構成されることを特徴とする鍵登録装置。
【請求項８】
前記出力手段は、前記第１鍵データを暗号化して前記第１機器へ出力し、
前記第１機器は、暗号化された第１鍵データを受け取り、復号する
ことを特徴とする請求項７記載の鍵登録装置。
【請求項９】
前記出力手段は、前記第１鍵データを、ネットワークを介して前記第１機器へ送信し、
前記第１機器は、ネットワークを介して前記第１鍵データを受信する
ことを特徴とする請求項７記載の鍵登録装置。
【請求項１０】
前記鍵登録装置は、
前記第１機器を認証する認証手段を含み、
前記鍵データ生成手段は、前記認証手段による認証結果が成功の場合、前記第１鍵データを生成する
ことを特徴とする請求項７記載の鍵登録装置。
【請求項１１】
前記鍵データ生成手段は、前記識別子から前記第１鍵データを生成する関数を記憶しており、
前記鍵データ生成手段は、前記関数を読出し、読み出した関数に前記識別子を代入して前記第１鍵データを生成する
ことを特徴とする請求項７記載の鍵登録装置。
【請求項１２】
前記鍵登録装置は、ＩＣカードであり、携帯電話又は情報携帯端末に接続可能であり、
前記出力手段は、前記携帯電話又は前記情報携帯端末を介して前記第１機器へ出力する
ことを特徴とする請求項７記載の鍵登録装置。
【請求項１３】
第２機器が有する、第１機器と前記第２機器との間で認証を行うための第２鍵データと同一の第１鍵データを、前記第１機器に設定する鍵登録装置で用いられるプログラムであって、
前記第２機器に固有の識別子の入力を受け付ける入力ステップと、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第１鍵データを生成する鍵データ生成ステップと、
生成した前記第１鍵データを前記第１機器へ出力する出力ステップと
を含むことを特徴とするプログラム。
【請求項１４】
第２機器が有する、第１機器と前記第２機器との間で認証を行うための第２鍵データと同一の第１鍵データを、前記第１機器に設定する鍵登録装置で用いられる方法であって、

前記第２機器に固有の識別子の入力を受け付ける入力ステップと、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第１鍵データを生成する鍵データ生成ステップと、
生成した前記第１鍵データを前記第１機器へ出力する出力ステップと
を含むことを特徴とする方法。
【請求項１５】
第２機器が有する、第１機器と前記第２機器との間で認証を行うための第２鍵データと同一の第１鍵データを、前記第１機器に設定する鍵登録装置で用いられるプログラムを記憶している、コンピュータ読み取り可能な記録媒体であって、前記プログラムは、
前記第２機器に固有の識別子の入力を受け付ける入力ステップと、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第１鍵データを生成する鍵データ生成ステップと、
生成した前記第１鍵データを前記第１機器へ出力する出力ステップと
を含むことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、複数の機器間において暗号認証通信を行うシステムに関する。
【０００２】
【従来の技術】
近年、パッケージメディアやインターネット、放送を用いた様々な音楽、映像コンテンツ配信サービスが広がっている。こういったサービスに対応して、コンテンツの著作権保護者の意思を反映したコンテンツ保護技術が必要になる。コンテンツ著作権保護者の意思としては、（１）コンテンツ配信サービスを有料とし、コンテンツの配信契約を結んだユーザの宅内での個人使用に限定したい、（２）不特定多数者がアクセスできるインターネットへの送信は許可しない、などがある。
【０００３】
このような、コンテンツの著作権保護者の意思を実現するためのコンテンツ保護技術の１つに、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）と呼ばれる規格がある。ＤＴＣＰは、高速シリアルバス規格の１つのＩＥＥＥ１３９４により規定されるバスを介して配信されるデジタルコンテンツの保護規格である。ＤＴＣＰについては、非特許文献１に詳しい。
【０００４】
ＤＴＣＰでは、ＤＴＬＡ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｌｉｃｅｎｓｉｎｇ　Ａｄｍｉｎｉｓｔｒａｔｏｒ，ＬＬＣ）と呼ばれる管理者の管理下でＤＴＣＰ規格に準拠した機器を相互接続し、その間で暗号認証通信を行っている。その仕組みを以下に示す。
（１）送信機器及び受信機器は、ＤＴＬＡから配布された秘密鍵を備えている。この秘密鍵の配布はＤＴＬＡとの契約に基づいて機器に配布される。なお、この秘密鍵の配布を受けた機器は、秘密鍵の管理実装方法を規定される。また、コンテンツのインターネットへの送信はＤＴＣＰの契約で禁止されている。
【０００５】
（２）送信機器と受信機器とは、上記秘密鍵を用いて相互認証を行う。また、送信機器は、保護が必要となるコンテンツを、認証により共有した鍵で暗号化して送信する。
（３）送信機器は、最大６３台までの受信機器にコンテンツを復号するための鍵を与える。ＩＥＥＥ１３９４のＡＶＣコマンドの制限及び台数制限により、コンテンツの個人使用限定を容易に実現する。
【０００６】
次に、Ｋｅｒｂｅｒｏｓ（ケルベロス）を利用した認証システムの概略を説明する。Ｋｅｒｂｅｒｏｓについては、非特許文献２に詳しい。

Ｋｅｒｂｅｒｏｓでは、正規の機器は予めＫｅｒｂｅｒｏｓサーバに登録されているとする。一例としてコンテンツの利用を受ける際、機器はまず、Ｋｅｒｂｅｒｏｓサーバにアクセスし、登録している情報を元に１回目の認証を受けて、Ｋｅｒｂｅｒｏｓサーバによりその日有効なチケット（イニシャルチケット）を獲得する。次に、機器は、当該サービスを提供するサーバにアクセスし、先にＫｅｒｂｅｒｏｓサーバからもらったイニシャルチケットを提示して、２回目の認証を受け、コンテンツを利用する。

【０００７】

このように、Ｋｅｒｂｅｒｏｓでは、認証を２回に分けて行うことにより、登録されている機器は、決められている有効期限内であればどのサービスも自由に利用することが出来る。

【０００８】

【非特許文献１】

「５Ｃ Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｗｈｉｔｅ Ｐａｐｅｒ」Ｒｅｖｉｓｉｏｎ１．０ Ｊｕｌｙ １４，１９９８

【０００９】

【非特許文献２】

ブライアン・タン著、桑村潤訳「ＫＥＲＢＥＲＯＳ ネットワーク認証システム」ピアソン出版、１９９９

【００１０】

【発明が解決しようとする課題】

しかしながら、上記何れの方法でも、宅内機器と宅外機器とを区別し、コンテンツの配信契約を結んだユーザ宅内での個人使用に限定できない。

そこで本発明はかかる問題点に鑑みてなされたものであり、コンテンツをユーザ宅内での個人使用に限定するために、ユーザ宅内の機器を簡易に設定することが可能な、認証システム及び鍵登録装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記目的を達成するために、本発明は、第１機器と第２機器との間において、認証を行う認証システムであって、前記第２機器に固有の識別子の入力を受け付け、所定の鍵生成アルゴリズムに基づいて前記識別子から第１鍵データを生成し、生成した第１鍵データを前記第１機器に送信する鍵登録装置と、前記鍵登録装置から前記第１鍵データを受信して記憶し、当該第１鍵データを用いて前記第２機器を認証する第１機器と、前記識別子から前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成される第２鍵データを予め記憶しており、前記第２鍵データを用いて前記第１機器による認証を受ける第２機器とから構成されることを特徴とする認証システムである。

【００１２】

この構成によると、鍵登録装置を用いない限り、第１機器に第２機器の鍵を登録することは出来ないので、登録された機器以外と通信することを防ぐ。これにより、コンテンツをユーザ宅内での個人使用に限定することが出来る。また、鍵登録装置を用いることによって、簡易に第１機器に第１鍵データを設定することが出来る。

【００１３】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

１．実施の形態１

１．１ 認証システム１１００の構成

認証システム１１００は、図１に示すように、専用端末１００、宅内システム２００及びコンテンツ配信装置８００から構成される。また、宅内システム２００は、宅内サーバ３００、ＴＶ４００、ＴＶ５００及びルータ６００から構成される。

【００１４】

コンテンツをユーザに有料で提供する管理機関９００は、専用端末１００、及びコンテン

ツ配信装置８００を有している。コンテンツ配信装置８００は、コンテンツを記録媒体に記録して提供する。なお、宅内システム２００とコンテンツ配信装置８００とが、ネットワークを介して接続されている場合、コンテンツをネットワークを介して配信しても良い。

ユーザは、自宅において、宅内システム２００を有している。

【００１５】

専用端末１００を所持しているサービスマンは、管理機関９００の指示により、ユーザの自宅を訪問し、専用端末１００を専用のインターフェースを介して宅内サーバ３００に接続する。なお、専用端末１００は、ＵＳＢなどの汎用のインターフェースを介して接続するようにしても良い。

専用端末１００は、外部からＴＶ４００に固有のＩＤである、機器識別子ＩＤ４の入力を受け付けると、機器識別子ＩＤ４から認証鍵Ｋｅｙ１４を生成する。生成した認証鍵Ｋｅｙ１４及び機器識別子ＩＤ４を宅内サーバ３００へ送信する。宅内サーバ３００は、機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を対応付けて記憶する。

【００１６】

一方、ＴＶ４００は、認証鍵Ｋｅｙ１４を予め記憶している。ユーザがＴＶ４００により、コンテンツを再生する際に、宅内サーバ３００は、ＴＶ４００を、認証鍵Ｋｅｙ１４を用いて認証し、宅内サーバ３００は、認証に成功した場合にコンテンツをＴＶ４００へ送信し、ＴＶ４００は、コンテンツを受信して再生する。

こうしてユーザは、コンテンツを楽しむことが出来る。

【００１７】

以下に、認証システム１１００の各構成について詳しく説明する。

１．１．１　専用端末１００

専用端末１００は、宅内サーバ３００にＴＶ４００の機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を登録するための装置である。専用端末１００は、管理機関９００から指示を受けたサービスマンが所持する。サービスマンは、ＴＶ４００が宅内に存在することを確認する。確認した後に、予め定められたコンテンツ保護機能を有する機器間でコンテンツを利用できるように、専用端末１００を用いて設定する。

【００１８】

専用端末１００は図２に示すように、制御部１０１、入力部１０２、検証部１０３、記憶部１０４、暗号化部１０５、鍵生成部１０６、送受信部１０７及び認証部１０８から構成される。

以下に、各構成について説明する。

（１）記憶部１０４

記憶部１０４は、サービスマン識別子ＩＤ＃Ｓ１、パスワードＳ１及び関数Ｆを記憶している。また、記憶部１０４は関数Ｆを用いて機器識別子Ｉ.Ｄ４を暗号化するための暗号化鍵Ｆ１を記憶している。

【００１９】

ここで、関数Ｆは一例としてＤＥＳの暗号化アルゴリズムである。ＤＥＳについては公知であるので、説明を省略する。

サービスマン識別子ＩＤ＃Ｓ１は、専用端末１００を利用するサービスマンに固有のＩＤである。パスワードＳ１は、専用端末１００を利用するためのパスワードであり、前記サービスマンのみがこのパスワードを知っている。

【００２０】

このサービスマン識別子ＩＤ＃Ｓ１及びパスワードＳ１によって、専用端末１００を使用できるサービスマンを限定する。

（２）入力部１０２

入力部１０２は、サービスマンの操作により、サービスマン識別子ＩＤ＃Ｓ１、パスワードＳ１及び機器識別子ＩＤ４の入力を受け付ける。受け付けたデータを制御部１０１に出力する。

（３）検証部１０３
検証部１０３は、以下のようにして、専用端末１００の使用を許可されたサービスマンであるか否かを検証する。
【００２１】
検証部１０３は、制御部１０１からサービスマンのサービスマン識別子ＩＤ#Ｓ１及びパスワードＳ１を受け取ると、記憶部１０４に記憶しているＩＤ及びパスワードを読み出す。受け取ったサービスマン識別子ＩＤ#Ｓ１及びパスワードＳ１と、読み出したＩＤ及びパスワードとが一致するか否かを検証する。検証結果を制御部１０１に出力する。
（４）認証部１０８
認証部１０８は、宅内サーバ３００と相互認証を行う。相互認証は、一例として、共通の情報を用いたチャレンジレスポンス方式で行う。ここで、チャレンジレスポンス方式については、公知であるので説明を省略する。
【００２２】
認証部１０８は、認証結果を制御部１０１に出力する。
（５）鍵生成部１０６
鍵生成部１０６は、制御部１０１から機器識別子ＩＤ４を受け取ると、記憶部１０４から関数Ｆを読み出す。読み出した関数Ｆを用いて機器識別子ＩＤ４から認証鍵Ｋｅｙ１４を生成する。
【００２３】
ここで、Ｋｅｙ１４＝Ｆ（Ｆ１，ＩＤ４）と表される。Ｆ（Ａ，Ｂ）は、暗号化鍵Ａを用いてＢを暗号化することを示す。
生成した認証鍵Ｋｅｙ１４を制御部１０１へ出力する。
（６）暗号化部１０５
暗号化部１０５は、暗号化鍵Ｅ１を有する。
【００２４】
暗号化部１０５は、制御部１０１から機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を受け取る。受け取った機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を、暗号化アルゴリズムＥに基づいて暗号化し、暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を生成する。ここで、暗号化機器識別子ＩＤ４＝Ｅ（Ｅ１，ＩＤ４）と表される。また、暗号化認証鍵Ｋｅｙ１４＝Ｅ（Ｅ１，Ｋｅｙ１４）と表される。Ｅ（Ａ，Ｂ）は、暗号化鍵Ａを用いて、Ｂを暗号化することを示す。
【００２５】
暗号化アルゴリズムＥは一例としてＲＳＡである。ＲＳＡは公知であるので説明を省略する。
暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を制御部１０１へ出力する。（７）送受信部１０７
送受信部１０７は、宅内サーバ３００とデータの送受信を行う。送受信部１０７は、制御部１０１から暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を受け取ると、宅内サーバ３００に送信する。
（８）制御部１０１
制御部１０１は、入力部１０２からサービスマン識別子ＩＤ#Ｓ１及びパスワードＳ１を受け取ると、受け取ったサービスマン識別子ＩＤ#Ｓ１とパスワードＳ１とを検証部１０３に検証させる。検証部１０３から検証結果を受け取る。検証結果が成功か否かを判断し、検証結果が失敗の場合、処理を終了する。検証結果が成功の場合、処理を継続する。
【００２６】
制御部１０１は、入力部１０２から機器識別子ＩＤ４を受け取ると、認証部１０８に宅内サーバ３００との相互認証を行わせる。認証部１０８から認証結果を受け取る。受け取った認証結果が成功か否かを判断し、認証結果が失敗の場合、処理を終了する。認証結果が成功の場合、鍵生成部１０６に機器識別子ＩＤ４を出力し、鍵を生成させる。鍵生成部１０６から認証鍵Ｋｅｙ１４を受け取ると、受け取った認証鍵Ｋｅｙ１４及び機器識別子Ｉ

Ｄ４を暗号化部１０５へ出力する。
【００２７】
暗号化部１０５から受け取る暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を、送受信部１０７を介して宅内サーバ３００に送信する。
１．１．２　宅内サーバ３００
宅内サーバ３００は、管理機関９００に認可された機器である。宅内サーバ３００は、蓄積コンテンツを記憶している。専用端末１００によって登録された鍵を用いて、ＴＶ４００又はＴＶ５００を認証し、蓄積コンテンツを配信する。
【００２８】
宅内サーバ３００は図２に示すように、制御部３０１、認証部３０２、送受信部３０３、復号部３０４、記憶部３０５、送受信部３０６、認証部３０７及び暗号化部３０８から構成される。
以下、各部について説明する。
（１）記憶部３０５
記憶部３０５は、記憶領域３０９及び外部からは観測や変更が出来ない領域である記憶領域３１０から成る。
【００２９】
記憶領域３０９は、蓄積コンテンツを記憶している。
記憶領域３１０は、既に登録されているＴＶ５００の機器識別子ＩＤ５及び認証鍵Ｋｅｙ１５を対応付けて記憶している。また、専用端末１００から受け取る、ＴＶ４００の機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を記憶する領域を備える。
（２）送受信部３０３
送受信部３０３は、専用端末１００と物理的に接続される。また、接続された専用端末１００とデータの送受信を行う。
（３）認証部３０２
認証部３０２は、専用端末１００と相互認証を行う。相互認証は、一例として共通の情報を用いたチャレンジレスポンス方式で行う。認証結果を制御部３０１に出力する。
（４）復号部３０４
復号部３０４は、制御部３０１から受け取る暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を、復号アルゴリズムＤに従って復号し、機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を生成する。ここで、復号アルゴリズムＤは、暗号化アルゴリズムＥの逆の処理を行う。
【００３０】
復号部３０４は、機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を制御部３０１へ出力する。
（５）送受信部３０６
送受信部３０６は、ルータ６００を介してＴＶ４００又は５００とデータの送受信を行う。
（６）認証部３０７
認証部３０７は、ＴＶ４００にコンテンツを配信する際、機器識別子ＩＤ４と認証鍵Ｋｅｙ１４を用いてＴＶ４００の認証及びセッション鍵の共有を行う。
【００３１】
認証及びセッション鍵共有の一例として以下の方法がある。
認証部３０７は、乱数ｒ１を生成し、ＴＶ４００に送信する。その後、ＴＶ４００から、ｒ１と、ＴＶ４００が生成した乱数ｒ２とを結合したデータｒ１ｒ２を、認証鍵Ｋｅｙ１４を用いて暗号化した暗号化ｒ１ｒ２を受信する。受信した暗号化ｒ１ｒ２を復号する。復号文からもとのｒ１が導出されることにより、ＴＶ４００を認証する。
【００３２】
また、このとき導出されたｒ２をセッション鍵として暗号化部３０８へ出力する。
認証部３０７は、ＴＶ５００にコンテンツを配信する際も同様の認証及びセッション鍵の共有を行う。

（７）暗号化部３０８
暗号化部３０８は、記憶領域３０９に記憶しているコンテンツを暗号化する。
【００８３】
ＴＶ４００へ配信するコンテンツは、認証部３０７でＴＶ４００を認証した際に導出されたセッション鍵ｋ２を用いて暗号化し、暗号化コンテンツを生成する。暗号化コンテンツを、制御部３０１へ出力する。
ＴＶ５００へ配信するコンテンツも、同様に導出したセッション鍵を用いて暗号化する。
（８）制御部３０１
制御部３０１は、専用端末１００が接続されると、認証部３０２に相互認証を行わせる。認証部３０２から認証結果を受け取る。認証結果が成功か否かを判断する。認証結果が失敗の場合、処理を終了する。認証結果が成功の場合、処理を継続する。制御部３０１は、送受信部３０３を介して専用端末１００から暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を受け取る。受け取った暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を復号部３０４に出力し、復号させる。
【００８４】
制御部３０１は、復号部３０４から復号した機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を受け取る。受け取った機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を対応付けて、記憶領域３１０に書き込む。
制御部３０１は、ＴＶ４００にコンテンツを配信する場合、認証部３０７でＴＶ４００の認証を行わせる。認証部３０７から認証結果を受け取ると、認証結果が成功か否かを判断する。認証結果が失敗の場合、コンテンツの配信を終了する。認証結果が成功の場合、暗号化部３０８にコンテンツを暗号化させる。暗号化部３０８から暗号化コンテンツを受け取ると、送受信部３０６を介してＴＶ４００へ配信する。
また、ＴＶ５００へコンテンツを配信する場合も同様の処理を行う。
１．１．３　ＴＶ４００，５００
ＴＶ４００，５００は、予め管理機関９００に認可された機器である。
【００８５】
ＴＶ４００は、外部から見ることが出来る場所に、管理機関９００が設定した、ＴＶ４００に固有の機器識別子ＩＤ４が付されている。
ＴＶ４００は図３に示すように、制御部４０１、認証部４０２、送受信部４０３、復号部４０７、記憶部４０４、モニタ４０５及びスピーカ４０６から構成される。また、ＴＶ５００も同様の構成である。なお、図３では簡単のため、宅内サーバ３００と、ルータ６００と、ＴＶ４００とを一列にして示す。
【００８６】
以下、各構成について説明する。
（１）記憶部４０４
記憶部４０４は、外部から観測や変更が出来ない記憶領域である。記憶部４０４は、ＴＶ４００に固有の機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を記憶している。認証鍵Ｋｅｙ１４は、機器識別子ＩＤ４から秘密の関数Ｆを用いて生成したものである。（２）認証部４０２
認証部４０２は、宅内サーバ３００と相互認証を行う。
【００８７】
認証部４０２は、送受信部４０３を介して乱数ｒ１を受け取ると、記憶部４０４から認証鍵Ｋｅｙ１４を読み出す。認証部４０２は、乱数ｒ２を生成する。受け取ったｒ１と生成したｒ２とを結合する。結合したデータｒ１ｒ２を、読み出した認証鍵Ｋｅｙ１４を用いて暗号化し、暗号化ｒ１ｒ２を生成する。暗号化ｒ１ｒ２を送受信部４０３を介して宅内サーバ３００に送る。
【００８８】
認証部４０２は、生成した乱数ｒ２をセッション鍵として復号部４０７に出力する。
認証部４０２は、認証結果を制御部４０１へ出力する。

（３）復号部４０７
復号部４０７は、送受信部４０３を介して暗号化コンテンツを受け取る。受け取った暗号化コンテンツを、認証部４０２で生成したセッション鍵Ｋ２を用いて復号する。復号したコンテンツを制御部４０１に出力する。
（４）モニタ４０５
モニタ４０５は、制御部４０１から受け取る画像データを再生する。
（５）スピーカ４０６
スピーカ４０６は、制御部４０１から受け取る音声データを再生する。
（６）送受信部４０３
送受信部４０３は、ルータ６００を介して、宅内サーバ３００と、データの送受信を行う。
（７）制御部４０１
制御部４０１は、認証部４０２に、送受信部４０３を介して宅内サーバ３００との相互認証を行わせる。認証部４０２から認証結果を受け取ると、認証結果が成功か否かを判断する。認証結果が失敗の場合、処理を終了する。
【００３９】
制御部４０１は、送受信部４０３を介して宅内サーバ３００から受信する暗号化コンテンツを、復号部４０７に復号させる。復号部４０７から復号されたコンテンツを受け取ると、モニタ４０５及びスピーカ４０６へ出力する。
１．２　認証システム１１００の動作
１．２．１　専用端末１００を用いて宅内サーバ３００にＴＶ４００を登録する場合の動作
以下、図４を用いて、専用端末１００を保持したサービスマンが宅内システム２００の宅内サーバ３００に、ＴＶ４００を登録する際の動作を説明する。ただし、宅内サーバ３００には、既にＴＶ５００が登録されている。
【００４０】
サービスマンは、専用端末１００を保持してユーザの宅内へ行く。コンテンツの利用が、個人使用の範囲として許容される場合、サービスマンは、ＴＶ４００が宅内にあることを確認して、登録の処理を行う。
サービスマンは、宅内サーバ３００に登録を行う前に、入力部１０２からサービスマンのサービスマン識別子ＩＤ#Ｓ１及びパスワードＳ１を入力する。専用端末１００の制御部１０１は、入力部１０２で入力を受け付けると、検証部１０３に検証させる。制御部１０１は、検証部１０３から検証結果を受け取ると、検証結果が成功か否かを判断する。検証結果が失敗の場合、登録処理を終了する。検証結果が成功の場合、登録処理を継続する。
【００４１】
専用端末１００は、サービスマンにより宅内サーバ３００に接続される。制御部１０１は、入力部１０２が機器識別子ＩＤ４の入力を受け付けると（ステップＳ１）、認証部１０８に、宅内サーバ３００と相互認証を行わせる（ステップＳ２）。制御部１０１は、認証部１０８から認証結果を受け取ると、認証結果が成功か否かを判断する（ステップＳ３）。認証結果が失敗の場合（ステップＳ３でＮＯ）、処理を終了する。認証結果が成功の場合（ステップＳ３でＹＥＳ）、鍵生成部１０６に鍵を生成させる（ステップＳ４）。制御部１０１は、鍵生成部１０６から生成された認証鍵Ｋｅｙ１４を受け取ると、機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を、暗号化部１０５に暗号化させる（ステップＳ５）。制御部１０１は、暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を、送受信部１０７を介して宅内サーバ３００に送信する（ステップＳ６）。
１．２．２　宅内サーバ３００が鍵を登録する場合の動作
宅内サーバ３００が、専用端末１００から受信した情報を書き込む際の動作を、図５を用いて説明する。
【００４２】
宅内サーバ３００の制御部３０１は、認証部３０２で専用端末１００と相互認証を行う（

ステップＳ１１）。制御部３０１は、認証部３０２から認証結果を受け取ると、成功か否かを検証し（ステップＳ１２）、検証結果が失敗の場合（ステップＳ１２でＮＯ）、処理を終了する。検証結果が成功の場合（ステップＳ１２でＹＥＳ）、専用端末１００からデータが送信されるのを待つ。

【００４３】

制御部３０１は、専用端末１００から送受信部３０３を介して、暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を受信する（ステップＳ１３）。暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ１４を復号部３０４で復号させる（ステップＳ１４）。復号した機器識別子ＩＤ４及び認証鍵Ｋｅｙ１４を対応付けて、記憶領域３１０に書き込む（ステップＳ１５）。

１．２．３　宅内サーバ３００がＴＶ４００にコンテンツを配信する際の動作

宅内サーバ３００が、ＴＶ４００にコンテンツを配信する際の動作を、図６を用いて説明する。

【００４４】

宅内サーバ３００の制御部３０１は、認証部３０７にＴＶ４００を認証させる（ステップＳ２１）。

制御部３０１は、認証部３０７から認証結果を受け取り、認証結果が成功か否かを判断する（ステップＳ２２）。認証結果が失敗の場合（ステップＳ２２でＮＯ）、処理を終了する。認証結果が成功の場合（ステップＳ２２でＹＥＳ）、記憶領域３０９に記憶している蓄積コンテンツを読み出す（ステップＳ２３）。読み出したコンテンツを、認証の際に導出したセッション鍵を用いて暗号化部３０８で暗号化する（ステップＳ２４）。暗号化したコンテンツを送受信部３０６を介してＴＶ４００に配信する（ステップＳ２５）。

１．２．４　宅内サーバ３００がＴＶ４００の認証を行う際の動作

宅内サーバ３００がＴＶ４００の認証を行う動作（ステップＳ２１）を、図７を用いて説明する。

【００４５】

宅内サーバ３００の認証部３０７は、乱数ｒ１を生成する（ステップＳ３１）。生成した乱数ｒ１を送受信部３０６を介してＴＶ４００に送信する（ステップＳ３２）。

ＴＶ４００の認証部４０２は、送受信部４０３を介して乱数ｒ１を受け取ると、乱数ｒ２を生成する（ステップＳ３３）。受け取ったｒ１と生成したｒ２を結合し（ステップＳ３４）、結合したｒ１ｒ２を、認証鍵Ｋｅｙ１４を用いて暗号化する（ステップＳ３５）。暗号化ｒ１ｒ２を送受信部４０３を介して宅内サーバ３００へ送信する（ステップＳ３６）。

【００４６】

宅内サーバ３００の認証部３０７は、受け取った暗号化ｒ１ｒ２を認証鍵Ｋｅｙ１４を用いて復号し、ｒ１ｒ２を導出する（ステップＳ３７）。復号したデータから、ｒ１が導出されたか否かを判断する（ステップＳ３８）。ｒ１が導出されなかった場合（ステップＳ３８でＮＯ）、認証が失敗であることを示す認証結果を制御部３０１へ出力する（ステップＳ４０）。ｒ１が導出された場合（ステップＳ３８でＹＥＳ）、暗号化部３０８へｒ２を出力する（ステップＳ３９）。また、認証部３０７は、認証が成功であることを示す認証結果を制御部３０１へ出力する（ステップＳ４０）。

２．実施の形態２

実施の形態１の方法では、鍵を登録した専用端末をサービスマンが紛失したときなど、不正に使用される可能性がある場合に、紛失前に登録されたものと、紛失後に登録されたものとが区別できないという問題がある。そこで、不正に使用される可能性がある専用端末で登録した鍵を無効化することが出来る認証システム１２００について説明する。

２．１　認証システム１２００の構成

認証システム１２００は、図８に示すように、専用端末１２０、１４０、宅内システム２２０、インターネット７００、管理装置９２０及びコンテンツ配信装置８００から構成される。また、宅内システム２２０は、宅内サーバ３２０、ＴＶ４２０、ＴＶ５２０及びル

ータ６２０から構成される。
【００４７】
管理装置９２０及びコンテンツ配信装置８００は、インターネット７００を経由して、ルータ６２０に接続されている。
以下、認証システム１１００と異なる構成について説明する。
２．１．１　管理装置９２０
管理装置９２０は、無効化情報を発行する。無効化情報は、不正利用される可能性がある専用端末及び当該専用端末で登録された鍵を無効化するための情報である。無効化情報は、無効化される専用端末に固有のＩＤと、ＩＤに対してデジタル署名アルゴリズムＳを施して生成したデジタル署名データから構成される。ここで、デジタル署名アルゴリズムＳは、一例として、有限体上の離散対数問題を安全性の根拠とするＥｌＧａｍａｌ署名方式に基づくものである。この有限体上のＥｌＧａｍａｌ署名方式については、公知であるので説明を省略する。
２．１．２　専用端末１２０
専用端末１２０は図１５に示すように、制御部１２１、入力部１２２、検証部１２３、記憶部１２４、暗号化部１２５、鍵生成部１２６、送受信部１２７及び認証部１２８から構成される。入力部１２２、検証部１２３、鍵生成部１２６、送受信部１２７及び認証部１２８は、専用端末１００と同様の構成である。
【００４８】
以下、専用端末１００と異なる構成の記憶部１２４、暗号化部１２５及び制御部１２１について説明する。
（１）記憶部１２４
記憶部１２４は、関数Ｆ、サービスマン識別子ＩＤ＃Ｓ２、パスワードＳ２及び、専用端末１２０に固有のＩＤであるＭｏｄｕｌｅ－２を記憶している。
（２）暗号化部１２５
暗号化部１２５は、制御部１２１から機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を受け取る。受け取った機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を、暗号化アルゴリズムＥに基づいて暗号化し、暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を生成する。暗号化部１２５は、暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を制御部１２１へ出力する。
（３）制御部１２１
制御部１２１は、専用端末１００の制御部１０１と同様に、検証部１２３にサービスマンのＩＤ及びパスワードを検証させ、認証部１２８に宅内サーバ３２０との相互認証を行わせ、鍵生成部１２６に鍵を生成させる。
【００４９】
制御部１２１は、鍵生成部１２６から認証鍵Ｋｅｙ２４を受け取ると、記憶部１２４からＭｏｄｕｌｅ－２を読み出す。機器識別子ＩＤ４及び受け取った認証鍵Ｋｅｙ２４と読み出したＭｏｄｕｌｅ－２とを暗号化部１２５に暗号化させる。
暗号化部１２５から暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を受け取ると、送受信部１２７を介して宅内サーバ３２０へ送信する。
２．１．３　専用端末１４０
専用端末１４０は図１６に示すように、制御部１４１、入力部１４２、検証部１４３、記憶部１４４、暗号化部１４５、鍵生成部１４６、送受信部１４７及び認証部１４８から構成される。
【００５０】
入力部１４２、検証部１４３、暗号化部１４５、送受信部１４７及び認証部１４８は、専用端末１２０と同様の構成のため、説明を省略する。
以下、専用端末１２０と異なる記憶部１４４、鍵生成部１４６及び制御部１４１について説明する。

（１）記憶部１４４
記憶部１４４は、関数Ｆと異なる関数Ｇ、サービスマン識別子ＩＤ#Ｓ３、パスワードＳ３及び専用端末１４０に固有のＩＤであるＭｏｄｕｌｅ－３を記憶している。
（２）鍵生成部１４６
鍵生成部１４６は、制御部１４１から機器識別子ＩＤ４を受け取ると、記憶部１４４から関数Ｇを読み出す。読み出した関数Ｇを用いて機器識別子ＩＤ４から認証鍵Ｋｅｙ３４を生成する。生成した認証鍵Ｋｅｙ３４を制御部１４１へ出力する。機器識別子ＩＤ５を受け取った場合も同様に処理し、認証鍵Ｋｅｙ３５を制御部１４１へ出力する。
（３）制御部１４１
制御部１４１は、制御部１２１と同様に、検証部１４３にサービスマン識別子ＩＤ#Ｓ３及びパスワードＳ３を検証させ、認証部１４８に宅内サーバ３２０との相互認証を行わせ、鍵生成部１４６に鍵を生成させる。
【００５１】
制御部１４１は、鍵生成部１４６から認証鍵Ｋｅｙ３４を受け取ると、記憶部１４４からＭｏｄｕｌｅ－３を読み出す。機器識別子ＩＤ４及び受け取った認証鍵Ｋｅｙ３４と読み出したＭｏｄｕｌｅ－３とを暗号化部１４５に暗号化させる。
暗号化部１４５から暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ３４及び暗号化Ｍｏｄｕｌｅ－３を受け取ると、送受信部１４７を介して宅内サーバ３２０へ送信する。
２．１．４　宅内サーバ３２０
宅内サーバ３２０は図１７に示すように、制御部３２１、認証部３２２、送受信部３２３、復号部３２４、記憶部３２５、送受信部３２６、認証部３２７、暗号化部３２８及び署名検証部３２９から構成される。
【００５２】
以下、宅内サーバ３００と異なる構成である記憶部３２５、署名検証部３２９及び制御部３２１について説明する。
（１）記憶部３２５
記憶部３２５は、図９に示すように、記憶領域３３２及び外部から観測や変更が出来ない領域である記憶領域３３０と記憶領域３３１とから成る。
【００５３】
記憶領域３３２は、コンテンツ配信装置８００から配信される蓄積コンテンツを記憶する領域である。
記憶領域３３１は、管理装置９２０の公開鍵を記憶している。
記憶領域３３０は図９に示すように、記憶領域３３３と３３４とから成る。
記憶領域３３４は、無効化された専用端末のＩＤを記憶する領域である。
【００５４】
記憶領域３３３は、既に宅内サーバ３２０に登録されているＴＶ５２０の機器識別子ＩＤ５、認証鍵Ｋｅｙ２５、Ｍｏｄｕｌｅ－２及び無効化フラグを対応付けて記憶している。Ｍｏｄｕｌｅ－２は、認証鍵Ｋｅｙ２５を登録した専用端末１２０のＩＤである。無効化フラグは、認証鍵Ｋｅｙ２５を登録した専用端末及び当該専用端末を用いて登録された鍵が無効化されているか否かを示すフラグである。図９では破線で囲んで示している。本実施の形態２では、無効化フラグが「１」の場合、対応付けられているＩＤが示す専用端末及び当該専用端末を用いて登録した鍵は無効化されていることを示し、「０」の場合、無効化されていないことを示す。
【００５５】
記憶領域３３３は、制御部３２１から受け取る機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を無効化フラグの「０」と対応付けて、図１０に示すように、記憶する。
（２）署名検証部３２９
署名検証部３２９は、制御部３２１から無効化情報を受け取る。受け取った無効化情報の管理機関９００の署名データに署名検証Ｖを施して検証する。ここで、署名検証Ｖは、前

記デジタル署名アルゴリズムＳにより生成された署名データを検証するアルゴリズムである。検証結果を制御部３２１へ出力する。

（３）制御部３２１

制御部３２１は、専用端末１２０から暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を受け取り、制御部３０１と同様に、復号部３２４で復号する。復号部３２４から機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を受け取ると、これらと無効化フラグの「０」とを対応付けて、図１０に示すように、記憶領域３３３に書き込む。

【００５６】

制御部３２１は、ルータ６２０を介して管理装置９２０から無効化情報を受信すると、署名検証部３２９に署名検証させる。署名検証部３２９から検証結果を受け取ると、検証結果が正しいか否かを判断する。検証結果が正しくない場合、処理を終了する。検証結果が正しい場合、受け取った無効化情報に含まれる無効化される専用端末のＩＤを、図１１に示すように、記憶領域３３４に記憶する。また、記憶領域３３３に記憶している鍵と対応付けて記憶しているＭｏｄｕｌｅ－２が、無効化情報に含まれるＩＤと一致するか否かを判断する。一致する場合、Ｍｏｄｕｌｅ－２と対応付けて記憶している無効化フラグ「０」を、図１１に示すように、「１」に書き換える。このように、無効化フラグ「１」と対応付けて記憶している認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ２５は、無効化されたことを示す。

【００５７】

また、制御部３２１は、Ｍｏｄｕｌｅ－２と対応付けて記憶している認証鍵Ｋｅｙ２４が無効化されたことを通知する認証鍵無効化情報を、送受信部３２６を介してＴＶ４２０及びＴＶ５２０に送信する。認証鍵無効化情報は、無効化されたＭｏｄｕｌｅ－２と対応付けて記憶している認証鍵Ｋｅｙ２４が無効化されたことを、ＴＶ４２０及びＴＶ５２０に通知するものであり、無効化された認証鍵Ｋｅｙ２４を含む。

２．１．５　ＴＶ４２０、５２０

ＴＶ４２０、５２０は、予め管理機関９００に認可された機器である。

【００５８】

ＴＶ４２０は図１８に示すように、制御部４２１、認証部４２２、送受信部４２３、復号部４２７、記憶部４２４、モニタ４２５及びスピーカ４２６から構成される。また、ＴＶ５２０も同様の構成であり、図１９に示すように、制御部５２１、認証部５２２、送受信部５２３、記憶部５２４、モニタ５２５、スピーカ５２６及び復号部５２７から構成される。送受信部４２３、復号部４２７、モニタ４２５及びスピーカ４２６は、ＴＶ４００と同様の構成である。以下、ＴＶ４００と異なる構成である記憶部４２４、認証部４２２及び制御部４２１について説明する。

（１）記憶部４２４

記憶部４２４は、外部から観測や変更が出来ない記憶領域である。記憶部４２４は、ＴＶ４２０に固有の機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ３４を記憶している。認証鍵Ｋｅｙ２４は、機器識別子ＩＤ４から関数Ｆを用いて生成した鍵である。認証鍵Ｋｅｙ３４は、機器識別子ＩＤ４から関数Ｇを用いて生成した鍵である。認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ３４には、予め優先順位が決められている。認証鍵Ｋｅｙ２４は、認証鍵Ｋｅｙ３４より優先順位が上位であり、先に利用される。

【００５９】

ＴＶ５２０の記憶部５２４も同様に、機器識別子ＩＤ５、認証鍵Ｋｅｙ２５及び認証鍵Ｋｅｙ３５を記憶している。認証鍵Ｋｅｙ２５は、機器識別子ＩＤ５から関数Ｆを用いて生成したものであり、認証鍵Ｋｅｙ３５は、機器識別子ＩＤ５から関数Ｇを用いて生成したものである。認証鍵Ｋｅｙ２５及び認証鍵Ｋｅｙ３５にも、優先順位が決められている。

（２）認証部４２２

認証部４２２が認証部４０２と異なる部分について説明する。

【００６０】

認証部４２２は、宅内サーバ３２０により認証を受けるとき、優先順位が上位の認証鍵Ｋｅｙ２４を先に用いて、ｒ１ｒ２を暗号化する。認証鍵Ｋｅｙ２４が無効化された場合は、次の優先順位の認証鍵Ｋｅｙ３４を用いる。

（３）制御部４２１

制御部４２１は、送受信部４２３を介して宅内サーバ３２０から認証鍵無効化情報を受信すると、記憶部４２４に記憶している認証鍵Ｋｅｙ２４又は認証鍵Ｋｅｙ３４の何れかと一致するか否かを判断する。一致する場合、一致した認証鍵を削除する。

２．２　認証システム１２００の動作

２．２．１　専用端末１２０を用いて宅内サーバ３２０にＴＶ４２０を登録する場合の動作

宅内サーバ３２０とＴＶ５２０とが、ルータ６２０で接続されている宅内システム２２０に、サービスマンが新たにＴＶ４２０を接続して、宅内サーバ３２０に鍵を設定する際の動作を説明する。ただし、ＴＶ５２０の鍵認証鍵Ｋｅｙ２５は、宅内サーバ３２０にすでに登録されている。

【００６１】

サービスマンは、専用端末１２０を保持してユーザ宅内へ行く。サービスマンは、登録処理を行う前に、専用端末１２０に、サービスマン識別子ＩＤ＃Ｓ２及びパスワードＳ２を入力する。

専用端末１２０の制御部１２１は、入力部１２２からサービスマンのサービスマン識別子ＩＤ＃Ｓ２及びパスワードＳ２の入力を受け付けると、専用端末１００と同様に、検証部１２３に検証させる。制御部１２１は、検証部１２３から検証結果を受け取ると、検証結果が成功か否かを判断する。検証結果が失敗の場合、登録処理を終了する。検証結果が成功の場合、登録処理を継続する。

【００６２】

専用端末１２０は、サービスマンにより、宅内サーバ３２０に接続される。制御部１２１は、入力部１２２で機器識別子ＩＤ４の入力を受け付けると、実施の形態１と同様の動作で認証鍵Ｋｅｙ２４を生成する。制御部１２１は、鍵生成部１２６から認証鍵Ｋｅｙ２４を受け取ると、記憶部１２４からＭｏｄｕｌｅ－２を読み出す。機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を暗号化部１２５へ出力する。

【００６３】

暗号化部１２５は、受け取った機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を、暗号化アルゴリズムＥに基づいて暗号化する。暗号化部１２５は、暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を制御部１２１へ出力する。

制御部１２１は、受け取った暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を、送受信部１２７を介して宅内サーバ３２０へ送信する。

【００６４】

宅内サーバ３２０の制御部３２１は、送受信部３２３を介して暗号化機器識別子ＩＤ４、暗号化認証鍵Ｋｅｙ２４及び暗号化Ｍｏｄｕｌｅ－２を受け取ると、実施の形態１と同様に復号部３２４に復号させる。

制御部３２１は、復号部３２４から復号した機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を受け取ると、記憶領域３３４から無効化した専用端末のＩＤを読み出す。読み出したＩＤと、復号したＩＤとが一致するか否かを判断する。一致する場合、処理を終了する。一致しない場合又は記憶領域３３４にＩＤが記憶されていない場合、制御部３２１は、図１０に示すように、Ｍｏｄｕｌｅ－２と機器識別子ＩＤ４と認証鍵Ｋｅｙ２４と無効化フラグ「０」と対応付けて記憶領域３３３に書き込む。

２．２．２　専用端末１２０が無効化された場合の動作

専用端末１２０が、紛失等で不正に利用される可能性がある場合に、専用端末１２０を無効化する動作を、図１３を用いて説明する。

【００６５】

管理装置９２０は、無効化情報をインターネット７００を介して、宅内サーバ３２０に配信する。
宅内サーバ３２０の制御部３２１は、ルータ６２０及び送受信部３２６を介して無効化情報を受信する（ステップＳ４１）。受信した無効化情報の署名データを署名検証部３２９で検証する（ステップＳ４２）。
【００６６】
制御部３２１は、署名検証部３２９から検証結果を受け取る。受け取った検証結果が正しいか否かを判断する（ステップＳ４３）。検証結果が正しくない場合（ステップＳ４３でＮＯ）、処理を終了する。検証結果が正しい場合（ステップＳ４３でＹＥＳ）、図１１に示すように、無効化情報に含まれる専用端末１２０のＩＤであるＭｏｄｕｌｅ－２を記憶領域３３４に書き込む（ステップＳ４４）。また、記憶領域３３３に記憶している鍵認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ２５を生成した専用端末１２０のＩＤであるＭｏｄｕｌｅ－２を読み出す（ステップＳ４５）。読み出したＭｏｄｕｌｅ－２と、無効化情報に含まれるＩＤとが一致するか否かを判断する（ステップＳ４６）。一致しない場合（ステップＳ４６でＮＯ）、処理を終了する。一致する場合（ステップＳ４６でＹＥＳ）、図１１に示すように、記憶領域３３３に記憶しているＭｏｄｕｌｅ－２を用いて登録した認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ２５を無効化するため、対応して記憶している無効化フラグを「１」に書き換える（ステップＳ４７）。
【００６７】
また、制御部３２１は、認証鍵Ｋｅｙ２４が無効化されたことを通知する認証鍵無効化情報を、送受信部３２６を介してＴＶ４２０及びＴＶ５２０に送信する。
このように、宅内サーバ３２０は、無効化された専用端末１２０のＩＤであるＭｏｄｕｌｅ－２を登録することで、無効化された専用端末１２０からの接続を拒否する。また、認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ２５を無効化することで、専用端末１２０を用いて不正に設定されても、不正に設定されたＴＶとの認証及びコンテンツの利用を拒否する。
２．２．３　専用端末１４０でＴＶ４２０及びＴＶ５２０を再登録する場合の動作
関数Ｆで生成された鍵認証鍵Ｋｅｙ２４及び認証鍵Ｋｅｙ２５が無効化された後、サービスマンが、ＴＶ４２０及びＴＶ５２０のもう一つの鍵認証鍵Ｋｅｙ３４及び認証鍵Ｋｅｙ３５を、別の専用端末１４０を用いて再登録する。
【００６８】
サービスマンは、専用端末１４０を保持してユーザ宅内へ行く。サービスマンは、登録処理を行う前に、専用端末１４０に、サービスマン識別子ＩＤ#Ｓ３及びパスワードＳ３を入力する。
専用端末１４０の制御部１４１は、入力部１４２からサービスマンのサービスマン識別子ＩＤ#Ｓ３及びパスワードＳ３の入力を受け付けると、専用端末１００と同様に、検証部１４３に検証させる。制御部１４１は、検証部１４３から検証結果を受け取ると、検証結果が成功か否かを判断する。検証結果が失敗の場合、登録処理を終了する。検証結果が成功の場合、登録処理を継続する。
【００６９】
専用端末１４０は、サービスマンにより、宅内サーバ３２０に接続される。制御部１４１は、入力部１４２で機器識別子ＩＤ４の入力を受け付けると、専用端末１００と同様の動作で、関数Ｇを用いて鍵認証鍵Ｋｅｙ３４を生成する。制御部１４１は、暗号化部１４５で専用端末１４０のＩＤであるＭｏｄｕｌｅ－３、機器識別子ＩＤ４、生成した鍵認証鍵Ｋｅｙ３４を暗号化させる。暗号化Ｍｏｄｕｌｅ－３、暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ３４を、送受信部１４７を介して宅内サーバ３２０に送信する。制御部１４１は、機器識別子ＩＤ５の入力を受け付けた場合も、同様に処理する。
【００７０】
宅内サーバ３２０の制御部３２１は、受け取った情報を復号部３２４で復号する。制御部３２１は、復号部３２４から受け取るＭｏｄｕｌｅ－３、機器識別子ＩＤ４及び認証鍵Ｋｅｙ３４と、無効化フラグ「０」とを対応付けて、図１２に示すように、記憶領域３３３

に書き込む。同様に、Ｍｏｄｕｌｅ－３、機器識別子ＩＤ５及び認証鍵Ｋｅｙ３５と、無効化フラグ「０」とを対応付けて、図１２に示すように、記憶領域３３３に書き込む。

３．実施の形態３

実施の形態２の認証システム１２００で鍵を再登録する際など、登録するＴＶが宅内にあり、管理機関９００から認可を受けていることを確認できる場合、サービスマンが宅内で設定せず、ネットワークを介して設定しても良い。

【００７１】

以下、専用端末１４０でインターネット７００を介して、宅内サーバ３２０に鍵を設定する場合の構成について説明する。

３．１　認証システム１３００の構成

認証システム１３００は、図１４に示すように、専用端末１２０，１４０、宅内システム２２０、インターネット７００、管理装置９２０及びコンテンツ配信装置８００から構成される。また、宅内システム２２０は、宅内サーバ３２０、ＴＶ４２０、ＴＶ５２０及びルータ６２０から構成される。

【００７２】

管理装置９２０、コンテンツ配信装置８００及び専用端末１４０は、インターネット７００を経由して、ルータ６２０に接続されている。

以下、認証システム１２００と異なる構成について説明する。

３．２　認証システムの動作

３．２．１　専用端末１４０で鍵を再登録する場合の動作

実施の形態２の方法で、専用端末１２０が無効化された後、宅内サーバ３２０に、インターネット７００を介して専用端末１４０を用いてＴＶ４２０の認証鍵Ｋｅｙ３４及びＴＶ５２０の認証鍵Ｋｅｙ３５を再登録する場合の動作について説明する。

【００７３】

管理機関９００は、ユーザから電話で、ＴＶ４２０の機器識別子ＩＤ４を知らせてもらう。なお、ＩＤ４を知らせてもらう方法は、電話に限らず電子メールなどでも良い。

サービスマンは、サービスマン識別子ＩＤ＃Ｓ３及びパスワードＳ３を入力部１４２から入力する。

【００７４】

制御部１４１は、実施の形態２と同様にサービスマンのサービスマン識別子ＩＤ＃Ｓ３及びパスワードＳ３を検証する。

専用端末１４０は、サービスマンによってインターネット７００に接続されると、実施の形態１と同様の方法で、宅内サーバ３２０と相互認証を行う。相互認証が成功した場合、専用端末１４０と宅内サーバ３２０とを接続する安全な通信路を確保する。安全な通信路は、一例として、ＩＰＳｅｃ（ＩＰ　Ｓｅｃｕｒｉｔｙ）といった手法により、通信路上のデータが暗号化されていることで実現される。

【００７５】

管理機関９００で、サービスマンは、専用端末１４０の入力部１４２から機器識別子ＩＤ４を入力する。

専用端末１４０の制御部１４１は、入力部１４２から機器識別子ＩＤ４の入力を受け付けると、専用端末１２０と同様の動作で、関数Ｇを用いて認証鍵Ｋｅｙ３４を生成する。制御部１４１は、暗号化部１４５でＭｏｄｕｌｅ－３、機器識別子ＩＤ４、生成した認証鍵Ｋｅｙ３４を暗号化させる。制御部１４１は、暗号化Ｍｏｄｕｌｅ－３、暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ３４を、インターネット７００を介して、宅内サーバ３２０に送信する。制御部１４１は、機器識別子ＩＤ５の入力を受け付けた場合も、同様に処理する。

【００７６】

宅内サーバ３２０の制御部３２１は、暗号化Ｍｏｄｕｌｅ－３、暗号化機器識別子ＩＤ４及び暗号化認証鍵Ｋｅｙ３４を受け取ると、復号部３２４に復号させる。復号されたＭｏｄｕｌｅ－３、機器識別子ＩＤ４及び認証鍵Ｋｅｙ３４と、無効化フラグ「０」とを対応

付けて、記憶領域３３３に書き込む。また、暗号化Ｍｏｄｕｌｅ－３、暗号化機器識別子ＩＤ５及び暗号化認証鍵Ｋｅｙ３５を受け取ると、同様に復号し、Ｍｏｄｕｌｅ－３、機器識別子ＩＤ５及び認証鍵Ｋｅｙ３５と、無効化フラグ「０」とを対応付けて、記憶領域３３３に書き込む。

【００７７】

このように、専用端末１４０で、インターネット７００を介して、宅内サーバ３２０に鍵を設定することが可能である。

４．　その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）無効化情報は、インターネットを介して配信されるとしたが、ＤＶＤやＣＤ等の蓄積メディア媒体に記録されて通知されるようにしても良い。

【００７８】

また、この方法では、宅内サーバが、外部への接続手段を持たなくても実現できる。

（２）無効化された鍵を無効化フラグ「１」と対応付けて記憶するとしたが、これに限定されない。無効化された専用端末で登録された機器のＩＤ及び鍵が削除される等、利用できない状態にすれば良い。

（３）実施の形態３で、鍵を宅内サーバに再登録する際を例として説明したが、これに限らない。

【００７９】

宅内サーバに登録する機器が宅内にあり、管理機関９００に認可された機器であることを確認できれば、新しく登録する場合でも良い。宅内にあることを確認する方法の一例として、ユーザが機器を購入する際に、ユーザ登録カードとして、購入する機器を管理機関９００に登録しておき、これを利用する方法がある。また、機器のＩＤの一部がＴＶであることを示す等、何れの機器であるか判断できる場合は、管理機関９００から認可されている機種であるかを確認することが出来る。また、ＩＤの一部が、管理機関９００から認可されていることを示すようにしても良い。

（４）実施の形態３で、安全な通信路をＩＰＳｅｃとしたが、これに限定されず、一般的なＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）としてもよい。また、専用線を用いて物理的に安全であっても良い。

（５）実施の形態３で、専用端末１４０が暗号化したデータを宅内サーバ３２０に送信するとしたが、宅内サーバ３２０がルータ６２０を介して、専用端末１４０にデータを取りにいく構成であっても良い。

（６）専用端末は、ＩＣカードをＰＤＡ又は携帯電話に接続したものであっても良い。この場合、関数Ｆ、Ｇなど、ＩＤと鍵の対応関係をＩＣカードが記憶している。

（７）本実施の形態では、サービスマンが入力部からＴＶのＩＤを入力するとしたが、ＩＤがバーコードとしてＴＶに付されており、それを専用端末で読み取るようにしても良い。また、ＩＣチップ等に記録されており、専用端末で読み取るようにしても良い。

（８）ＩＤから鍵を生成する方法として、関数Ｆ又は関数Ｇを用いるとしたが、ＩＤと鍵の対応関係を示すものであれば関数でなくても良い。例えば、専用端末は、ＩＤと鍵との対応表を記憶している構成であっても良い。

（９）宅内サーバに鍵を登録する機器は、ＴＶでなくても良い。他の画像再生機器であっても良いし、音声再生機であっても良い。また、ＤＶＤやメモリカード等の蓄積メディアに書き込みを行う記録機器であっても良い。

【００８０】

宅内サーバは、ＤＶＤ等の蓄積メディアの再生機器であっても良い。

（１０）本実施の形態では、宅内サーバが、一つのＴＶにコンテンツを配信する方法を記述したが、同時に複数のＴＶにコンテンツを配信するようにしても良い。

ＴＶ４００とＴＶ５００にコンテンツを配信する際の相互認証の一例として、以下のような方法がある。

【００８１】
まず、実施の形態１と同様の方法で、それぞれのＴＶと相互認証を行う。次に、宅内サーバはコンテンツを暗号化するためのコンテンツ鍵を生成する。これを各ＴＶとそれぞれ共有したセッション鍵で暗号化して、暗号化コンテンツと共にそれぞれのＴＶに配信する。ＴＶは、暗号化コンテンツを、宅内サーバと共有したセッション鍵で復号する。復号したコンテンツ鍵で暗号化コンテンツを復号し、再生する。
【００８２】
これにより、複数のＴＶで同時にコンテンツを再生することが出来る。
（１１）本実施の形態では、宅内サーバがＴＶ４００を認証するとしたが、宅内サーバとＴＶとが相互認証を行う構成であっても良い。
（１２）本実施の形態２．３で、ＴＶは関数Ｆを用いて生成した鍵と、関数Ｇを用いて生成した鍵の２つを持つとしたが、鍵は３個以上でも良い。この場合、それぞれの鍵は、それぞれ別の関数を用いて、ＩＤから生成されたものである。
（１３）宅内サーバとＴＶは、ルータを介してイーサネット（登録商標）で接続されるとしたが、これに限らない。ローカルに設定されたシステムであっても良いし、ルータを用いなくても良い。
（１４）宅内サーバからコンテンツの配信を禁止する対象としては、ＰＣだけではなく、記録機器にも配信を禁止することが出来る。
【００８３】
また、上記の場合、以下に示すように送信制御をコンテンツの種類によって行っても良い。
宅内サーバは、登録する機器のＩＤや鍵と共に、その機器が視聴だけを目的とした機器であるか、記録を行うことを目的とした機器であるか、といった機器の種類を記憶しておく。そして、別途コンテンツに付加されているコピーコントロール情報を元にして、機器への配信を許可又は禁止する。ここで、コピーコントロール情報は、一般的に（１）ＣｏＰｙ　Ｎｅｖｅｒ、１回もコピーしてはいけない、（２）ＣｏＰｙ　Ｏｎｃｅ、１回だけコピーしても良い、（３）ＣｏＰｙ　Ｆｒｅｅ、自由にコピーしても良い、の３つの状態を区別する。宅内サーバは、コンテンツに付加されているコピーコントロール情報が（２）又は（３）の場合、記録機器へ配信可能と判断し、（３）の場合、コンテンツの配信を禁止する。
（１５）実施の形態２では、無効化情報を受信した宅内サーバ３２０は、ＴＶ４２０及び５２０に、認証鍵無効化情報を送信するとしたが、宅内サーバ３２０は、受け取った無効化情報をＴＶ４２０及び５２０に送信するとしても良い。
【００８４】
この構成の場合、認証鍵Ｋｅｙ２４を宅内サーバ３２０に登録する際、専用端末１２０から機器識別子ＩＤ４、認証鍵Ｋｅｙ２４及びＭｏｄｕｌｅ－２を受け取った宅内サーバ３２０は、Ｍｏｄｕｌｅ－２をＴＶ４２０に送信する。ＴＶ４２０は、受信したＭｏｄｕｌｅ－２と優先順位が上位の認証鍵とを対応付けて記憶する。ＴＶ５２０も同様の処理を行う。
【００８５】
宅内サーバ３２０は無効化情報を受信すると、受信した無効化情報をＴＶ４２０及び５２０に送信する。ＴＶ４２０及びＴＶ５２０は、優先順位が上位の認証鍵と対応付けて記憶しているＭｏｄｕｌｅ－２と、受信した無効化情報に含まれる無効化専用端末のＩＤとが一致するか否かを判断し、一致する場合、Ｍｏｄｕｌｅ－２を削除する。また、宅内の全ての機器が、管理装置９２０から無効化情報を受信し、受信した機器はそれぞれ、認証鍵の無効化を判断するようにしても良い。
（１６）実施の形態２では、ＴＶ４２０及び５２０は、認証鍵無効化情報を受信すると、認証鍵を削除するとしたが、本発明はこれに限定されない。認証鍵が無効化され、使用できないことを判断できれば良い。
【００８６】

例えば、予め認証鍵に無効化フラグを付しておき、認証鍵無効化情報を受信すると、認証鍵無効化情報に含まれる認証鍵と一致する認証鍵に付されている無効化フラグを、無効化に書き換える構成でも良い。

（１７）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【００８７】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【００８８】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【００８９】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（１８）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【００９０】

【発明の効果】

以上説明したように、本発明は、第１機器と第２機器との間において、認証を行う認証システムであって、前記第２機器に固有の識別子の入力を受け付け、所定の鍵生成アルゴリズムに基づいて前記識別子から第１鍵データを生成し、生成した第１鍵データを前記第１機器に送信する鍵登録装置と、前記鍵登録装置から前記第１鍵データを受信して記憶し、当該第１鍵データを用いて前記第２機器を認証する第１機器と、前記識別子から前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成される第２鍵データを予め記憶しており、前記第２鍵データを用いて前記第１機器による認証を受ける第２機器とから構成されることを特徴とする認証システムである。

【００９１】

また、本発明は、第１機器と第２機器との間において、認証を行う認証システムであって、前記第２機器に固有の機器識別子の入力を受け付け、鍵生成アルゴリズムに基づいて前記機器識別子から第１鍵データを生成し、生成した第１鍵データを前記第１機器に送信する鍵登録装置と、前記鍵登録装置から受信する前記第１鍵データを記憶し、前記第１鍵データを用いて前記第２機器を認証する第１機器と、前記機器識別子からそれぞれ異なる鍵生成アルゴリズムに従って生成される複数の鍵データを予め記憶しており、前記複数の鍵データの内、前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第２鍵データを選択し、選択した第２鍵データを用いて、前記第１機器による認証を受ける第２機器とから構成されることを特徴とする認証システムである。

【００９２】

また、本発明は、第２機器が有する、第１機器と前記第２機器との間で認証を行うための第２鍵データと同一の第１鍵データを、前記第１機器に設定する鍵登録装置であって、前記第２機器に固有の識別子の入力を受け付ける入力手段と、鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第１鍵データを生成する鍵データ生成手段と、生成した前記第１鍵データを前記第１機器へ出力する出力手段とから構成

されることを特徴とする鍵登録装置である。

【００９３】

この構成によると、鍵登録装置を用いない限り、第１機器に第２機器の鍵を登録することは出来ないので、登録された機器以外と通信することを防ぐ。これにより、コンテンツをユーザ宅内での個人使用に限定することが出来る。また、外部への接続手段を持たない機器でも実現できる。

ここで、前記第１機器は、更に、鍵登録装置の無効化を管理する管理機関により生成され、前記鍵登録装置の無効化を示す鍵無効化情報を受け取り、前記鍵登録装置から受信した第１鍵データを無効化し、前記第２機器は、前記鍵無効化情報を受け取り、前記第２鍵データを無効化するようにしても良い。

【００９４】

この構成によると、無効化された鍵登録装置で登録した鍵データは無効化されるので、不正に鍵登録装置を用いて鍵データが登録されても、無効化することが出来る。

ここで、前記認証システムは、更に、鍵再登録装置を含み、前記鍵再登録装置は、前記第２機器に固有の機器識別子の入力を受け付け、前記鍵登録装置の鍵生成アルゴリズムと異なる鍵生成アルゴリズムに基づいて前記第２機器に固有な機器識別子から第３鍵データを生成し、生成した第３鍵データと前記機器識別子とを前記第１機器に送信し、前記第１機器は、更に、前記鍵再登録装置から受信する前記第３鍵データ及び前記機器識別子を対応付けて記憶し、前記第３鍵データを用いて前記第２機器を認証し、前記第２機器は、更に、前記複数の鍵データの内、前記第３鍵データを生成した鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第４鍵データを用いて、前記第１機器による認証を受けるようにしても良い。

【００９５】

この構成によると、登録した鍵データが無効化されても、第２機器は複数の鍵データを持つので、正規の鍵再登録装置を用いることによって、第１機器に新たに鍵データを登録することが出来る。

ここで、前記第１機器は、前記管理機関により生成され、無効化された鍵登録装置に固有の識別子を更に含む鍵無効化情報を受け取り、更に受け取った識別子を無効化識別子として記憶し、鍵登録装置から、第１鍵データと共に、前記鍵登録装置に固有の識別子を受け取り、受け取った識別子が前記無効化識別子と一致するか否かを判断し、一致する場合、前記鍵登録装置から前記第１鍵データを受け取ることを拒否するようにしても良い。

【００９６】

この構成によると、第１機器は、無効化された鍵登録装置の識別子を無効化識別子として記憶しているので、無効化された鍵登録装置を用いて鍵データを登録しようとしても拒否し、不正に鍵データを登録することを防ぐことが出来る。

ここで、前記第１機器は、前記管理機関により生成され、前記鍵無効化情報に前記管理機関の署名を施して生成された署名データを更に含む前記鍵無効化情報を受け取り、前記署名データを検証し、検証結果が成功であれば、前記識別子を無効化識別子として記憶するようにしても良い。

【００９７】

この構成によると、第１機器は、鍵無効化情報に含まれる署名データの検証結果が成功の場合に、無効化識別子として記憶するので、前記管理機関によって発行されたことを確認することが出来、改ざんされているか否かを確認できる。これにより、不正に鍵データを登録されることを防ぐ。

ここで、前記出力手段は、前記第１鍵データを暗号化して前記第１機器へ出力し、前記第１機器は、暗号化された第１鍵データを受け取り、復号するようにしても良い。

【００９８】

また、前記鍵登録装置は、前記第１機器を認証する認証手段を含み、前記鍵データ生成手段は、前記認証手段による認証結果が成功の場合、前記第１鍵データを生成するようにしても良い。

この構成によると、鍵データの不正利用を防止し、正規の機器の鍵データを登録することが出来る。

【００９９】

ここで、前記出力手段は、前記第１鍵データを、ネットワークを介して前記第１機器へ送信し、前記第１機器は、ネットワークを介して前記第１鍵データを受信するようにしても良い。

この構成によると、ネットワークを介して鍵データを登録するので、サービスマンが鍵登録装置を持ってユーザ宅内に行かなくても、ネットワークに接続できる任意の場所から鍵データを登録することが出来る。

【図面の簡単な説明】

【図１】認証システム１１００の全体の構成を示すブロック図である。

【図２】専用端末１００及び宅内サーバ３００の構成を示すブロック図である。

【図３】宅内サーバ３００及びＴＶ４００の構成を示すブロック図である。

【図４】制御部１０１の動作を示すフローチャートである。

【図５】制御部３０１が鍵を登録する際の動作を示すフローチャートである。

【図６】制御部３０１がコンテンツをＴＶ４００に配信する際の動作を示すフローチャートである。

【図７】認証部３０７と認証部４０２との相互認証の際の動作を示すフローチャートである。

【図８】認証システム１２００の全体の構成を示すブロック図である。

【図９】記憶部３２５の内部の構成を示すブロック図である。

【図１０】認証鍵Ｋｅｙ１４を記憶した際の記憶領域３３０の内部の構成を示すブロック図である。

【図１１】専用端末１２０が無効化された際の記憶領域３３０の内部の構成を示すブロック図である。

【図１２】専用端末１４０で再登録した際の記憶領域３３０の内部の構成を示すブロック図である。

【図１３】制御部３２１の動作を示すフローチャートである。

【図１４】認証システム１３００の全体の構成を示すブロック図である。

【図１５】専用端末１２０の構成を示すブロック図である。

【図１６】専用端末１４０の構成を示すブロック図である。

【図１７】宅内サーバ３２０の構成を示すブロック図である。

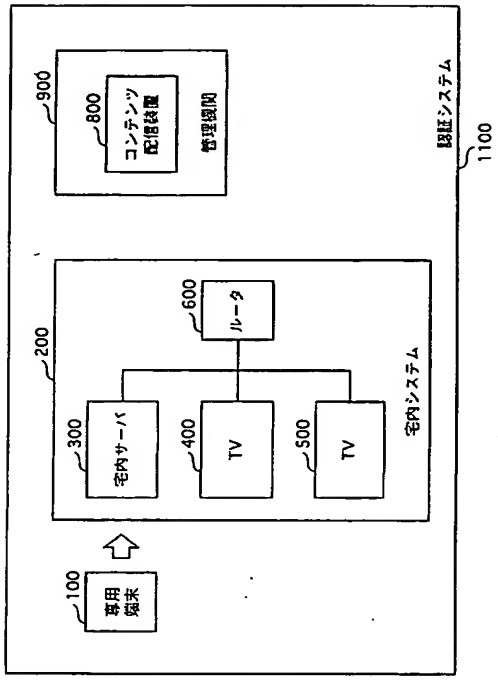
【図１８】ＴＶ４２０の構成を示すブロック図である。

【図１９】ＴＶ５２０の構成を示すブロック図である。

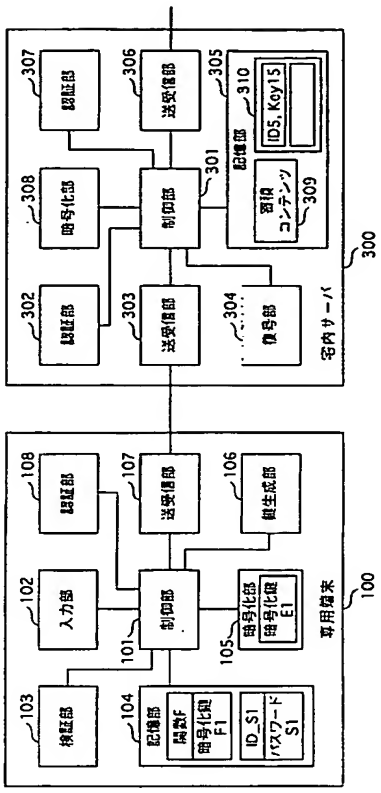
【符号の説明】

１００．１２０．１４０　専用端末
２００．２２０　宅内システム
３００．３２０　宅内サーバ
４００．４２０．５００．５２０　ＴＶ
６００．６２０　ルータ
７００　インターネット
８００　コンテンツ配信装置
９００　管理機関
９２０　管理装置
１１００　認証システム
１２００　認証システム
１３００　認証システム

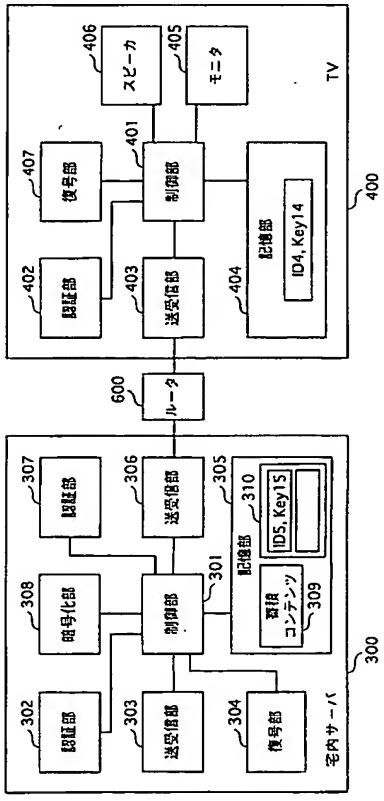
【図１】


認証システム
1100
管理機関
900
コンテンツ配信装置
800
宅内システム
200
ルータ
600
宅内サーバ
300
TV
400
TV
500
専用端末
100

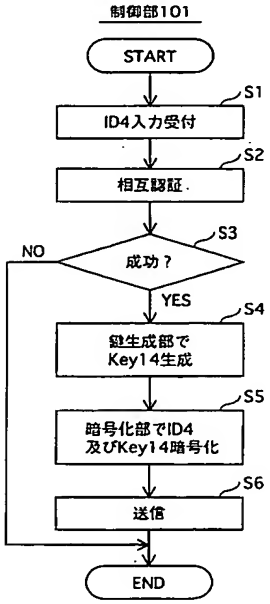
【図２】


宅内サーバ
300
認証部
307
送受信部
306
記憶部
305
ID5, Key15
310
制御部
301
暗号化部
308
蓄積コンテンツ
309
認証部
302
送受信部
303
復号部
304
専用端末
100
認証部
108
送受信部
107
生成部
106
入力部
102
制御部
101
暗号化部
105
暗号化鍵E1
検証部
103
記憶部
104
鍵対
暗号化鍵F1
ID_S1
パスワードS1

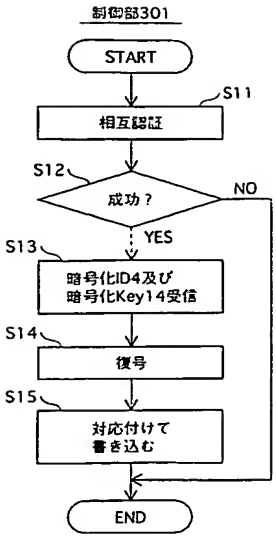
【図３】


TV
スピーカ
406
モニタ
405
制御部
401
復号部
407
認証部
402
送受信部
403
記憶部
404
ID4, Key14
400
ルータ
600
宅内サーバ
300
認証部
307
送受信部
306
記憶部
305
ID5, Key15
310
制御部
301
暗号化部
308
蓄積コンテンツ
309
認証部
302
送受信部
303
復号部
304

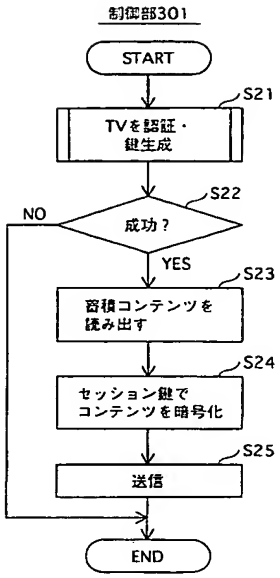
【図４】


制御部101
START
S1
ID4入力受付
S2
相互認証
S3
NO
成功？
YES
S4
生成部で
Key14生成
S5
暗号化部でID4
及びKey14暗号化
S6
送信
END

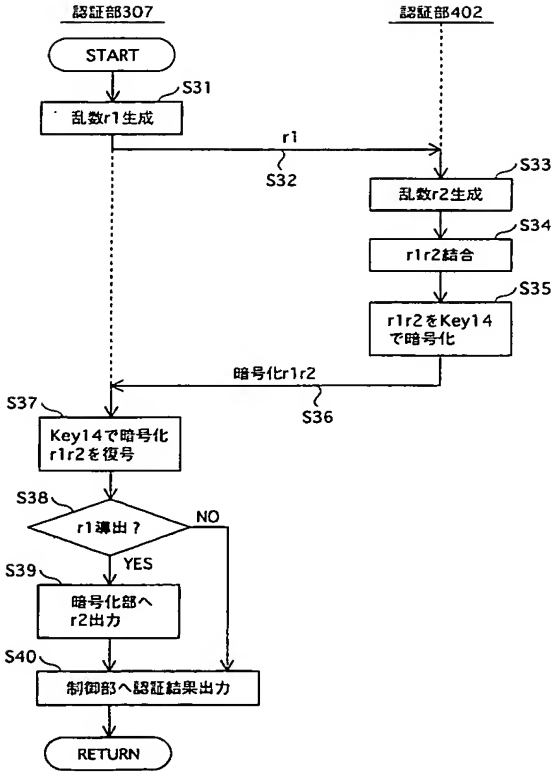
【図５】


制御部301
START
S11
相互認証
S12
成功？
NO
YES
S13
暗号化ID4及び
暗号化Key14受信
S14
復号
S15
対応付けて
書き込む
END

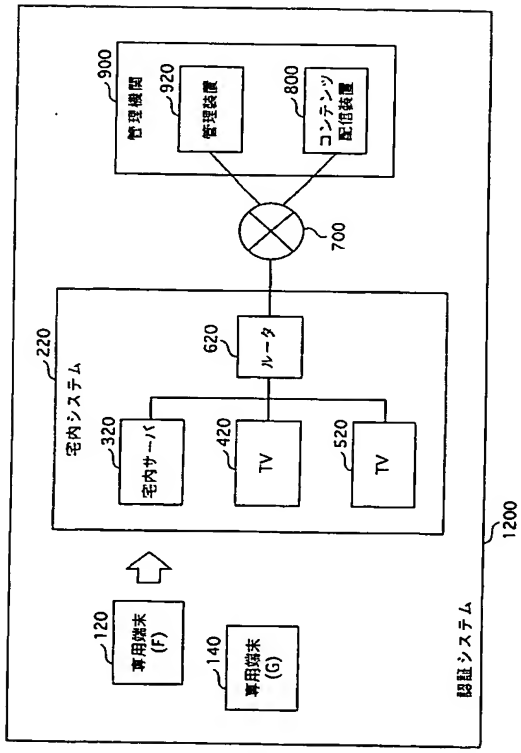
【図６】


制御部301
START
S21
TVを認証・
鍵生成
S22
成功？
NO
YES
S23
蓄積コンテンツを
読み出す
S24
セッション鍵で
コンテンツを暗号化
S25
送信
END

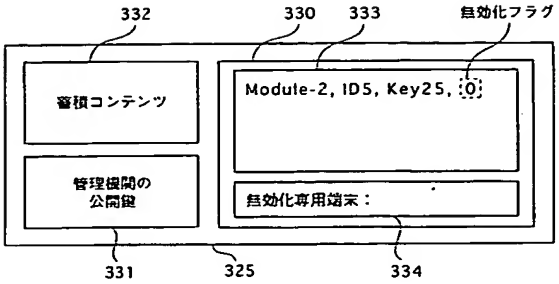
【図７】


認証部307
認証部402
START
S31
乱数r1生成
r1
S32
S33
乱数r2生成
S34
r1r2結合
S35
r1r2をKey14
で暗号化
暗号化r1r2
S36
S37
Key14で暗号化
r1r2を復号
S38
r1導出？
NO
YES
S39
暗号化部へ
r2出力
S40
制御部へ認証結果出力
RETURN

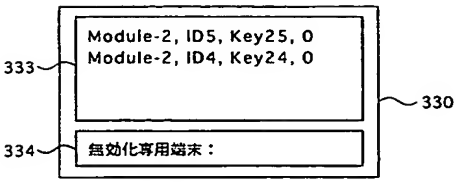
【図８】


900
管理機関
920
管理装置
800
コンテンツ
配信装置
700
220
宅内システム
620
ルータ
320
宅内サーバ
420
TV
520
TV
1200
120
専用端末
(F)
140
専用端末
(G)
認証システム

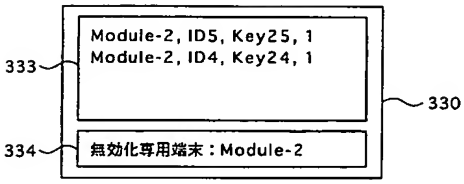
【図９】



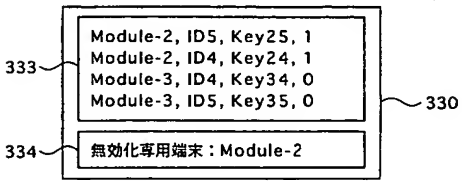
【図１０】



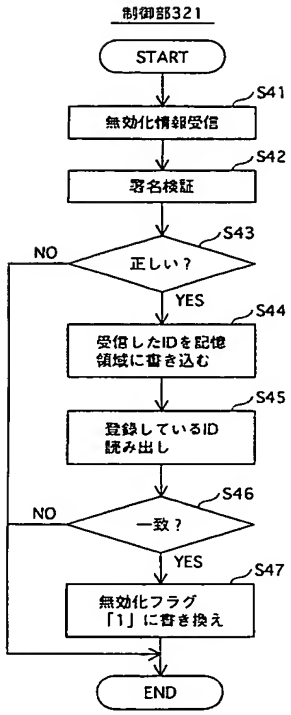
【図１１】



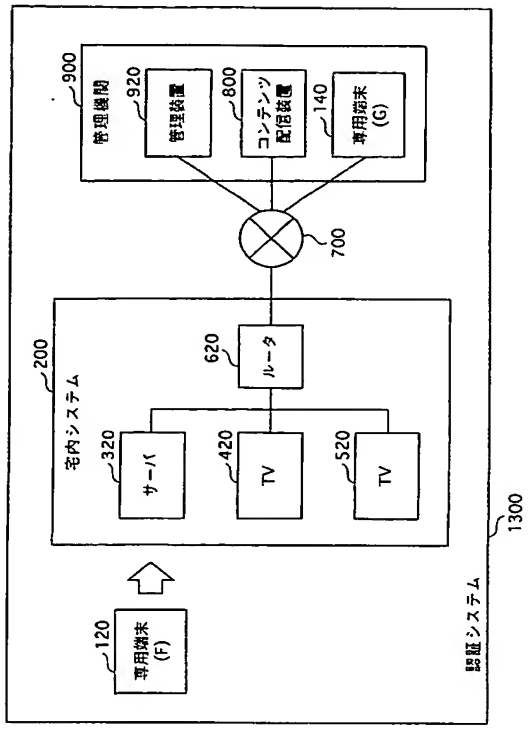
【図１２】



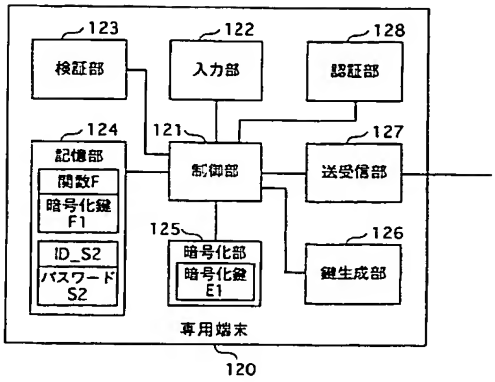
【図１３】



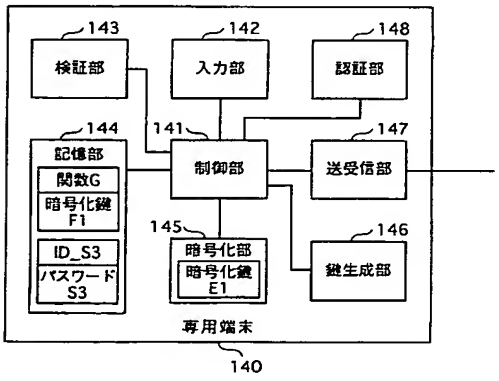
【図１４】



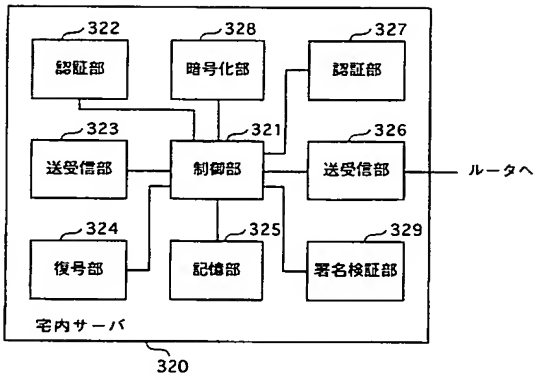
【図１５】



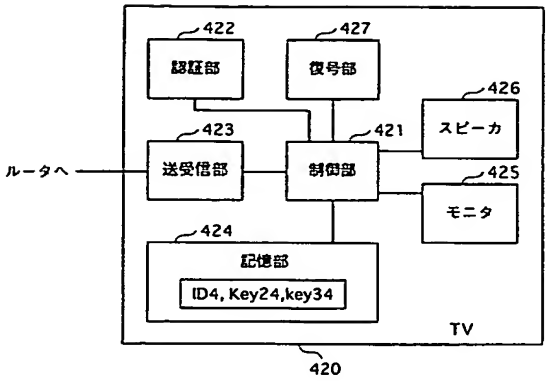
【図１６】



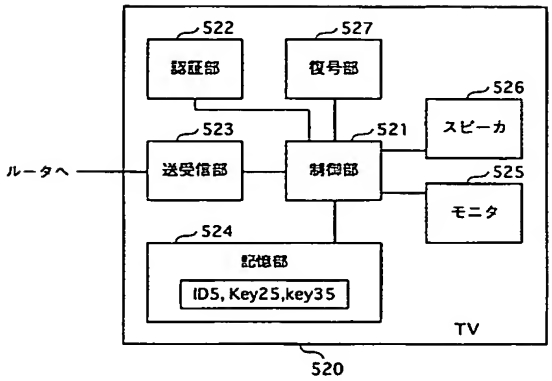
【図１７】



【図１８】


422
認証部
427
復号部
426
スピーカ
423
送受信部
421
制御部
425
モニタ
ルータへ
424
記憶部
ID4, Key24,key34
TV
420

【図１９】


522
認証部
527
復号部
526
スピーカ
523
送受信部
521
制御部
525
モニタ
ルータへ
524
記憶部
ID5, Key25,key35
TV
520

フロントページの続き

(72)発明者 布田 裕一
大阪府門真市大字門真１００６番地 松下電器産業株式会社内
(72)発明者 大森 基司
大阪府門真市大字門真１００６番地 松下電器産業株式会社内
(72)発明者 北虎 裕人
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

Fターム(参考) 5J104 AA07 AA12 AA16 AA34 EA04 EA15 EA16 EA18 JA03 JA21
JA29 KA02 KA04 KA06 KA15 MA05 NA02 NA05 NA27 NA35
NA37